Whitepaper

Protect

Google Workspace Data with Backup Solution

Use Google Workspace to store your crucial data, such as emails, contacts, notes, calendars, appointments, digital documents, etc. With the multiple-factor authentication feature, Google Workspace secures users' data in its cloud storage. However, users often accidentally delete their essential data or lose it in some scenarios, such as viruses & malware attacks. These scenarios may harm your Workspace data and corrupt them so users cannot access them. Follow this reliable guide to prevent your Google Workspace data from data loss or corruption.

The State of Data Protection: Industry Statistics

- According to the University of Texas, **94%** of organizations experience severe data loss and cannot recover them easily. In these **94%** of stats, **43%** of organizations never reopen, and **51%** permanently close within 2 years.

- As per an IBM survey, the average data breach cost in 2023 was 4.45 million. Thus, encrypting and securing is the only solution to safeguarding Workspace data.

Case in Point from an IT Admin

Mark, an IT admin, discovers that an employee has accidentally deleted his organization's Google Workspace data's project folder. The folder contains months of work, including emails, shared documents, and calendar events tied to deadlines.

Panic sets in when Mark realizes the data wasn't manually backed up. He needs to restore everything exactly as it was—folder structure, sharing permissions, etc.

The admin requested help from our Kernel Google Workspace Backup and Restore tool.

He selected the date before the deletion and began the backup process of the accidentally deleted file of the given dates.

With one click, he backed up the folder to its original state, including all sharing settings and permissions in the PST file.

After that, he restored that PST file in the selective Google Workspace account with ease.

What Challenges You May Face and Why Need Google Workspace Data Backup?

Due to limited data retention policies, accidental deletion, malicious attacks, and more, users may face a lot of challenges during Google Workspace data backup. An inside journey of IT Admin, Mark, shared a story of his employee who accidentally deleted a project folder in Google Workspace and how Kernel Google Workspace and Restore tool helped them to rescue data from deleted folder after retention period.

Check out full insights on how Mark escaped the data loss situation and got his backup. Read our whitepaper now and secure your Google Workspace data.

Limited time period for data backup: Google Workspace retains deleted data for only 25-30 days in the deleted or trash folder. Recovery is impossible after the retaining period without using an automated solution.

Third-Party App Vulnerabilities: Other integrated applications or add-ins with excessive permissions can lead to data breaches or unauthorized access without users' permission.

Malicious attacks (ransomware, phishing): Malicious attacks, such as ransomware and phishing, are serious cyber threats that abruptly damage data integrity and steal sensitive information from Workspace accounts.

Sync errors and data corruption: When your Workspace account faces sync errors and data corruption issues that can disrupt workflows, exploit your working experience, and lead to significant business losses.

Lack of inbuilt backup options: Google Workspace offers only a few inbuilt features to backup crucial data, such as Google Workspace Admin Export tool, Google Vault, and Google Takeout.

What are the steps to secure Google Workspace Data to Reduce Major Data Loss Risks?

Step 1: Risk assessment and data classification

Identify critical data and workflows: Know all the prominent risks and filter out your crucial data for backup, such as emails, documents, spreadsheets, presentations, and shared drives. Also, verify public, internal, and highly confidential data sensitivity levels.

Assessing potential risk: Evaluate potential risks, including accidental deletion, insider threats, or misuse of permissions of the Google Workspace data.

Step 2: Get Your Backup with Workspace's Built-in Tools

Using Google Workspace's built-in tools: Google Workspace offers several built-in backup tools, such as **Google Admin Export Tool**, **Google Vault**, and **Google Takeout**, that secure organizations' data.

Configuring Sharing and access controls: Securely access Workspace data to prevent unauthorized exposure. Restrict your file sharing to suspicious users or unauthorize domains.

Step 3: Why Need to Use the 3rd Party Backup Solutions?

While Google Workspace provides backup prevention features, it is not a substitute for comprehensive backups. Native tools like Google Vault are designed for retention and compliance, not for granular recovery. Kernel Google Workspace Backup and Restore software is a professional software that automates your Workspace data backup and restores them in any Google account.

Check out some advanced features of this software:

Automated Backups: Schedule single or multiple Google Workspace data backup to PST, MSG, and more formats in local or NAS Drive.

Data Restoration: Restore specific data from a PST file to a Workspace account with just a few clicks.

Compliance Ready: Meet the regulatory requirements of Google Workspace with ease.